Documentary script of The Lost Data

We're entering the Anonymous Literature documentary series. We the anonymous members are making it possible to search for the lost data but if not possible to recover it completely. Enjoy.

Anonymous Literature Media Productions.

The Lost Data

The question that we ask is; why are we losing data by deleting the data on our computers?

Another question is where does the deleted data go after emptying the trash from our computers?

If the trash is emptied from our computers, then our data will be lost forever, it doesn’t matter, from Microsoft, Apple Mac OS, or Linux OS’s, if we trash the important data from our computers by emptying the trash from our computers, then our data will be lost forever and it’s so irretrievable and irreplaceable plus it cannot be undone and it’s irreversible.

It is possible to retrieve the data if trashed on the computer by accident.

Do not lose your data, retrieve it if you need to, especially if

you’re censored.

Backup your data on an external hard drive instead of your local computer drive, cyber media platforms such as Facebook, and online cloud services such as Dropbox and iCloud.

If were locked out of our computers, then we may lose our data forever if we forgot our password.

Millions of people have lost their data on their computers due to censorship, the erasure of the computer, being locked out of the computer, hardware theft, computer viruses, hardware impairment, natural disasters, and power failure, the damage, made unreadable by users and software applications, erasure of the hard drive, reformatting the hard drive, not backing up the data, or corruption.

We all went through the technical mistake whether we lost the data or not.

Michael Stevens of Vsauce has asked a similar question about where did the deleted data go on his video from YouTube.

We’ll play some videos of Leo Notenboom of Ask Leo who was questioning about how to recover the data and stuff like his experiences.

Are we at risk of losing our digital information over time? The key here is to, for physical storage media, keep moving forward. Keep iterating forward to newer hardware that will continue to be supported for more years. Now, the other issue, of course, is the formats of the actual files. And this is actually a little bit trickier. Uh, I have a couple of different opinions on this. One is that every digital format can be figured out. It can be reverse engineered. It's just work. So if 10 years from now you have a file that is using an obscure file format, it would be possible to reverse engineer and transform that file into something else. Would it be worth it? I can't say. I'm sure that historians of the future may decide that, yeah, you know, that thing over there, that was so important that we really do need to reverse engineer and come up with a new interface that will read that file format. On the other hand, I am absolutely convinced that our most common file formats today: things like PDF, Zip, potentially even Word documents and Excel spreadsheets. These are so ubiquitous today that the ability to read them will be here for a very, very long time, probably a lot longer than the ability to create them, because we'll probably have moved on to something else. But because there's so much documentation, so much information that is stored in these formats, and because these formats are generally open, I see no reason that we couldn't always have a fairly easy way to at least read the information that's been stored in these files. All we're really talking about here is another form of backing up. Copying data forward, well, it's making a copy. You're stacking the deck in favor of using a newer

technology that will last, say, another 20 years or another 30 years. In another 20 years, you choose the format that at that point will last another 20 or 30 years. Now, one of the things that a lot of people don't think about is that this is not a new problem. Data preservation is absolutely nothing new. In the past, think about it. One of the things that monks did 500, 800 years ago was copy documents painstakingly by hand because the originals that they were working from were deteriorating. They very carefully made copies. That's where, to me, digital storage makes complete sense. Because what might have taken a monk a month to copy, again painstakingly by hand, can be copied in seconds and distributed around the world.

Quote, I lost a huge amount of research and work when my computer crashed this summer. That's a quote from an email that I got from someone who experienced exactly that. He is not the only one running the risk, the risk of massive data loss. Here's the thing. Imagine your computer gone, just literally gone. It could be stolen. It could be destroyed. The important thing is that everything stored on that computer has disappeared. Is that a problem? If that's a problem, if that's a catastrophe, then you are not protected and you should be and you can be. On the other hand, if it's an inconvenience, great. You're probably doing the things that need to be done to keep yourself safe. Quite honestly, is that it is so easy to prevent data loss.

First, do no harm. I'm not going to name the repair shop

because much of what I have is speculation, word of mouth, the results of my examining the external drive in question and so forth. I really don't know what it was they were given to begin with. One of the most important steps in any data recovery effort is to make sure you're not making matters worse. Many recovery techniques, if performed improperly or even if performed correctly, will actually alter the data stored on the drive in question. This then can overwrite other data that might be important for recovering other files. It's not a bad thing. It's just the nature of data recovery techniques. Knowing that, the first thing you should do is take steps to ensure that no matter what, you can always get back to where you were. The computer repair folks apparently failed to consider that. As a result, by the time I got to look at it, the disk had been manipulated extensively. I've been referring to it as having been stomped on. My chances of actually addressing the original problem were slim to none. The best I could hope for was some kind of partial recovery. So the lead up. How did we get here? The symptoms were actually really simple to begin with. Eight files suddenly appeared to be corrupt. They wouldn't open. That's it. Eight files out of several hundred or maybe a few thousand files stored on this external drive. My friend had been backing up manually, but the most recent was a couple of months ago. Naturally, there was important stuff on that drive that had been created or updated since then. When my friend got the drive back from the computer repair people, those eight files were back. Yay. except all the other files were gone. All of them. So they went back to the computer

repair shop and said, hey, what happened? Followed by some variation of get my files back. Now the computer repair folks attempted data recovery on the drive. The result was not pretty. The previous folder structure was completely lost. There were many duplicates of the recovered files, which is not uncommon for file recovery. Many of the recover files lost their file names, replaced by a generic file number type thing. Many files were incomplete or damaged, and many files were missing. And that's it. That's the best they could do. Only excuses were offered from that point. Anything not included in the above was lost. OK, great. You say do no harm. What was the shop supposed to have done? Well, the repair shop should at least have asked, is this drive backed up and take an appropriate action if the answer had been no. Heck, an experienced shop wouldn't even ask. They would assume the answer was no and take action anyway. Now, I've often pointed out that image backups on working systems make for a great checkpoint. No matter what you do after the backup, like installing or updating software or making other changes, you can always restore the backup and be back where you were with no harm done.

And you don't get to choose which failure you're going to have. Malware happens. It shouldn't. In a perfect world, there would be no malware. In a perfect world, our anti-malware tools would catch 100% of all malware destined for our machines. We don't live in a perfect world. Malware happens. Ransomware happens. You cannot avoid these scenarios. You can prepare for them. Here's what could have

happened. The hard disk dies, you replace it, you restore the previous day's image backup, and you get on with your life. It's that simple. It really is. Or perhaps the machine is infected and all the files are encrypted on it and a ransom is demanded. You restore the machine from the previous day's backup. You're done. You get on with your life. You learn from the experience, of course, so as not to repeat whatever caused the malware to arrive in the first place. This is why I harp so much about backing up. It is the closest thing to a silver bullet when you're faced with hardware failure, malware, basically any form of data loss.

I currently have images stored on memory cards, thumb drives, CDs and DVDs. Which is best long term? My off the cuff answer, probably none of the above. They all have a little bit of a problem. Optical media, CDs and DVDs, for example. Well, as it turns out, unless you've actually purchased archival quality, then they're fading as you sit. Over the years they will actually start to deteriorate and the result is that the data on those disks may no longer be recoverable. That's kind of scary and exactly what you don't want when it comes to archival media. Similarly, when it comes to any kind of flash memory, I'm going to start, though, with the inexpensive SD cards, micro SD cards, USB thumb drives. That kind of flash memory is typically relatively inexpensive and there's actually no good data that says it's going to last any length of time.

If it happens to you and you're not prepared, you're likely to

lose whatever was on that drive forever. 95% of it might be easily replaceable or irrelevant, but that last 5%, losing that can be extremely painful. And I've seen this over and over again. Start planning for the next time. Back up. Please don't tune out. I know I talk about this a lot, but that's because it's important. I keep running into situations exactly like this where everything would have been a complete non-issue had there been some kind of a backup in place. Planning for the next failure means planning for that failure to be a non-issue. Here's how you tell. Imagine your laptop, your computer, your cloud storage account just disappeared without notice and without hope of recovery. If that means you would lose important stuff, then you're not backed up. If it's in only one place, it's not backed up. So yeah, of course, how do I back up is usually the next question. There are so many different approaches to backing up. So, here are a few alternatives. Every so often, copy your important files somewhere else. An external hard disk is a great place to start. The more important the data, the more often you should make sure that that backup is up to date. Keep your important data in a cloud service like Dropbox or OneDrive or Google Drive or Proton Drive or any of many others. If you lose the account, the files are still on your PC. And if you lose the computer, the files are still online. Install a backup tool like Macrium Reflect or EaseUS Todo, have it make automated full image backups to your external hard disk periodically. While I greatly prefer that last one, and it's what I truly, truly recommend, any of those techniques, and probably several others, would be better than not backing

up at all. Backup, please.

Leo Notenboom, a founder of Ask Leo since 2003. Leo Notenboom was an expert in mainly data loss and data recovery.

We’re almost running out of storage on our computers and we are at risk of losing an important data.

If we run out of storage on our computers, then we’ll need more computers, storage upgrades on our computers, or get more external hard drives and we’ll never be at risk of losing a data ever again.

Cyber data

What is cyber data?

Cyber data refers to information stored or transmitted electronically, which can be vulnerable to threats like data loss. Data loss occurs when sensitive information is damaged, deleted, or made inaccessible, often due to cyberattacks or the systematic failures.

How does cyber data work?

Cyber data operates through several key processes: collection: data is gathered from various sources, including servers, applications, and user devices. This can involve logs

from firewalls, intrusion detection systems, and user activity. Analysis: collected data is analyzed to identify patterns and anomalies. This helps in detecting potential threats or breaches. Advanced techniques like machine learning and behavioral analytics are often used for deeper insights. Response: once threats are identified, organizations can take action. This may involve blocking malicious traffic, alerting security teams, or initiating incident response protocols.

Understanding how cyber data works is vital for effective cybersecurity management and protection against cyber threats.

Cyber data and digital data are 2 different terms but cyber data and digital data are often used interchangeably, but they can refer to different aspects. Cyber data typically relates to data involved in cybersecurity contexts, while digital data encompasses all forms of data stored or transmitted electronically.

Don’t lose cyber data and digital data, protect them and get ready for a backup.

Neutralizing the data loss

Why do we neutralize the data or the data loss? To make the data neutral and harmless plus we want to reduce the data loss.

It is sad to lose the important data cause it’s so irreplaceable plus we should save, recover, and neutralize it.

It's data versus information.

Big data? That’s similar to corporate data but we want the neutral data.

Neutralizing data can help reduce bias and improve the accuracy of predictions by removing the influence of certain features.

It’s important to neutralize data loss by implementing effective data protection strategies, such as regular backups, encryption, and employee training to recognize threats.

How to neutralize data loss? To neutralize data loss, implement a robust backup strategy that includes both online and offline backups, ensuring data is stored in multiple locations. Additionally, use encryption and access control measures to protect sensitive information from unauthorized access and accidental loss.

The cases of the lost data

Pixar Animation Studios

How did Pixar delete the data by accident and then recover it?

During the Toy Story 2 production, Pixar almost lost the Toy Story franchise due to a lack of data backup cause around 90% of the entire production files of Toy Story 2 were deleted by mistake. This resulted in character models and assets disappearing, and the file servers were quickly shut down. Pixar nearly lost millions of dollars for the data loss. This is a technical mistake.

After an emergency meeting of the executives of Pixar, and due to one lucky "work from home" stint, the files were recovered.

Going from Toy Story 2 being deleted to being rescued in such a short amount of time was no doubt nightmarish for those involved, especially the employee who typed the delete command, but at least it's a story with a neutral ending.

Internet Archive

Internet Archive has experienced a significant data loss due to some glitch that deleted many user accounts and associated data, including favorites and uploads. This incident has raised concerns about the reliability of the archive as a preservation resource.

Internet Archive had experienced the cyberattack, it was September to October 2024 and the internet archive has tried to recover the data but it did recover 99% of the data.

The Conscious Resistance Network

The Conscious Resistance Network focuses on empowering individuals through education and community organizing, but specific details about data loss are not provided in the available information.

The Conscious Resistance Network was experiencing the censorship on Youtube in 2020 or 2021 that lead to data loss but at least it recovered the data as The Conscious Resistance Network was back on Youtube.

The Corbett Report: Open Source Intelligence News

The Corbett Report, which is known for its alternative news and analysis, has faced censorship on Youtube but it got censored on Youtube due to the data loss in 2020 or 2021.

Lezley Saar & Agust Agustsson

Lezley saar didn’t completely lose her data but however, she did not remember how many folders were accidentally deleted on her Macbook Pro laptop recently.

We don’t know how much data that Agust Agustsson had lost on his computer due to some malware and or corruption.

Pits Data Recovery got so many cases of data loss on the devices such as the flash drive.

Easystore flash drive recovery case, data loss can be a frustrating experience, especially when you need to access important information from your flash drive. One of the most common reasons for data loss from flash drives is when the computer does not recognize the device. There are several causes why a USB device may stop being recognized by a computer due to a faulty USB cable or a malfunctioning USB port, due to a software issue, a corrupted driver, or a conflicting operating system update but it's actually beyond frustration cause of the snafu due to mainly the corruption. When a USB drive is not recognized, it is important to not panic. There are several things that you can try before resorting to a recovery company. The problem is with the USB port itself. If the flash drive is still not recognized on your computer, try plugging it into a different one. This will help you determine if the problem is with the flash drive or your computer's USB ports. The cable can be the culprit. If your flash drive is If your flash drive is an external hard drive or a USB drive with a detachable cable, try using another USB cable to connect it to your computer. A simple restart can solve the problem. Try restarting your computer with the flash drive plugged in to see if it's recognized. If none of the above solutions work, the flash drive may have the hardware issue. Check for any physical damage or wear and tear on the flash drive. If it's damaged, you may need to replace it.

Successful data recovery from a WD My Passport, data loss can occur on the external hard drives for some various reasons, including accidental deletion, water damage, disk management issues, physical impacts, or the malware attacks. The client discovered that the files on his WD My Passport were no longer accessible. While some files were still visible, he was unable to open them indicating that the data had become corrupted. The Pits Data Recovery team had opened it to investigate the issue that was caused by the physical damage and the signs of corrosion on the internal components, likely caused by the liquid exposure. It's the data loss situation. It's affecting the drive's read/write capabilities, leading to the data loss.

All data retrieved from the water-damaged MacBook Pro, spilling water on your MacBook Pro can be a nightmare. The thought of losing all your important files and documents can be overwhelming. However, there's still hope. With the right steps, you can recover your data. It is important to act quickly and follow the correct procedures to avoid permanent damage to your MacBook Pro. The client's data was lost. It's the best to seek professional data recovery services. They can ensure the safety and security of your data.

And many more cases of the data loss.

Microsoft and the lost data

What happens if you delete the whole Windows operating system?

If you delete the whole Windows operating system, your computer will no longer be able to boot up or run any applications as well as losing your data, as the OS is essential for managing hardware and software resources. You would need to reinstall an operating system to use the computer again.

Backup your data before reinstalling your Windows OS but if you don't, then you'll lose your data.

If you wish to permanently delete files, you will need to overwrite the data with special software if you have Windows OS. Always back up anything you do not wish to lose once the hard drive has been wiped clean, after which it will be impossible or very expensive to retrieve any lost data.

Data loss incidents can occur in Microsoft services, impacting organizations significantly. Understanding these events is crucial for implementing effective data protection strategies.

Microsoft had so many cases of data loss.

By understanding the risks and implementing robust data protection measures, organizations can mitigate the impact

of data loss incidents.

Apple and the lost data

Without having a Time Machine backup or any other backup of that data, you have lost all that data and it's a disaster.

What Happens If You Delete the Entire Macintosh HD?

If through reformatting, partition deletion, or other methods you completely erase your entire Macintosh HD drive, this will remove all data including the macOS system. The consequences include: Your Mac will fail to boot without a system to startup to. Booting will go to an emergency recovery partition or boot to internet recovery mode. All user data including documents, settings, apps, and media will be erased. The system will need to be reinstalled from macOS Recovery or an external boot drive. User data will need to be restored from a backup, if a backup exists. Erasing the entire Macintosh HD should only be done as part of a complete system reinstallation or when disposing of the Mac. Otherwise, data loss will occur. Have backups in place before fully erasing the drive.

How to recover your lost data from your Mac OS or iOS? Sometimes it can be impossible to recover the lost data without a backup.

Should we rely on Apple for the data recovery?

Apple devices can experience data loss due to various reasons, such as software updates or accidental deletions.

There are so many cases of data loss. Data breaches are a significant concern for Apple and its users, with millions of records compromised and substantial financial implications. Enhanced security measures are crucial to protect user data in an increasingly digital world.

A data breach can lead to data loss for Apple, as it may expose sensitive information stored in their systems. However, Apple implements strong security measures, including end-to-end encryption, to protect user data and minimize the risk of loss during such incidents.

Linux and the lost data

Erasing Linux from your computer will remove the operating system and any associated files, which may require you to delete specific partitions used by Linux plus you'll lose your data.

Data loss in Linux can occur due to various reasons such as hardware failures, accidental deletions, or malware. Implementing a robust backup strategy and using data recovery tools are essential to prevent and recover from data loss events.

Users of any Linux can significantly reduce the chances of data loss and ensure quick recovery when it occurs, especially reduce the data loss problems.

Is Linux immune to data loss? No, not completely but users of Linux can be at risk of certain things such as the data loss. Linux has the robust security features, vulnerabilities and risks still exist that can lead to data loss. Implementing data loss prevention (DLP) solutions can help mitigate these risks.

Future of data

How does the data affect the future? Data significantly influences the future by driving decision-making and innovation across various industries. As data volumes grow, organizations can leverage advanced analytics and technologies like the so-called artificial intelligence to gain insights that shape strategies and improve outcomes.

The future of data is focused on being unified, flexible, and accessible, allowing these organizations to extract valuable insights and drive innovation. As the technologies like the so-called artificial intelligence and real-time analytics evolve, the businesses can make faster, data-driven decisions, enhancing their competitive advantage.

The future of data management

With the rapid pace of technological advancements and the growing demand for data-driven insights, the field of data management is poised for transformative changes.

This article delves into the key developments, shaping the future of the data management and what organizations can expect in the years to come.

In the future, never ever lose data again.

How do devices affect the data?

Any devices can affect the data usage by varying in how much the data they consume based on their functions and capabilities. For example, smart mobile phones and tablets are designed to use the data efficiently, but they can also connect to the internet constantly, leading to a higher data consumption, especially during the activities like streaming or downloading any content.

Don't lose your data on every device at any cost. It does not matter, every data recovery apps are expensive. It’s easier to lose the data on any device than to recover it on any device. It’s a technical mistake.

Devices refer to physical hardware that can perform tasks, such as computers, smartphones, and IOT devices, while data is the information processed or stored by these devices. Together, they enable various functionalities, from

communication to data analysis and automation.

Don’t lose your device and data, have it with you.

If one loses data on our devices, we lose everything.

Big data? It’s like big tech or big corporate tech.

Big data is not completely immune to data loss; it can be vulnerable to various risks such as cyberattacks, hardware failures, and human errors. Implementing effective backup strategies and security measures is essential to mitigate these risks.

Just because we slowly prevent data loss, it doesn’t mean that we completely stay away from big brother.

However, balancing the benefits of surveillance with privacy and security concerns remains a significant challenge when it comes to data.

Prepare to backup your data now.

The end